RECEIVED
CENTRAL FAX CENTER
OCT 2 3 2008

Amendments To The Specification

Please replace paragraph [19] in the specification page 9, with the following amended paragraph:

In order to accomplish the above-mentioned object, a rijndael block decryption method according to a ~~second~~ third embodiment of the present invention comprises the steps of if a two-clock round operation start signal and a round number signal are inputted from a round operation control unit after an encryption or decryption operation start signal and a mode signal are inputted through a bus, a round key generation unit of a round operation unit transforming a 128-bit input key into a 128-bit round key for decryption in accordance with a value of the mode signal inputted through the bus from a time when a first clock of the round operation start signal becomes `1`, and storing the 128-bit round key in an internal 128-bit round key register; if the two-clock round operation start signal and a bit selection signal are inputted from the round operation control unit, a shift/inverse-shift_row transform unit performing a byte-inverse-shift of upper 64-bit data of 128-bit input data inputted through the bus, and outputting the byte-inverse-shifted upper 64-bit data through a first multiplexer when the first clock becomes `1`, a substitution/inverse-substitution transform unit successively performing an inverse substitution of the upper 64-bit data, and outputting the inverse-substituted upper 64-bit data to a first demultiplexer, an add-round-key transform unit successively performing an addition of the upper 64-bit data outputted through a decryption output terminal of the first demultiplexer to an upper 64-bit round key generated by the round key generation unit, and outputting the added upper 64-bit data to a third demultiplexer, and a mix/inverse-mixcolumn transform unit successively performing an inverse mixcolumn of the added upper 64-bit data, outputting the inverse-mixcolumn-transformed upper 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed upper 64-bit data in a 64-bit data register; and when a second clock of the round operation start signal becomes `1`, the shift/inverse-shift_row transform unit performing a byte-inverse-shift of lower 64-bit data of the 128-bit input data inputted through the bus and outputting the byte-inverse-shifted lower 64-bit data through the first multiplexer, the substitution/inverse-substitution transform unit successively performing an inverse substitution of the lower 64-bit data, and outputting the inverse-substituted lower 64-bit data to the first demultiplexer, the add-round-key transform unit successively performing an addition of the lower 64-bit data outputted through the decryption output terminal of the first demultiplexer to a lower 64-bit round key generated by the round key generation unit, and outputting the added lower 64-bit data to the third demultiplexer, the mix/inverse-mixcolumn transform unit successively performing an inverse mixcolumn of the added lower 64-bit data, outputting the inverse-mixcolumn-transformed lower 64-bit data through a second demultiplexer, and storing the inverse-mixcolumn-transformed lower 64-bit data in lower 64 bits of a 128-bit data register, and simultaneously storing the upper 64-bit data stored in the 64-bit data register in upper

64 bits of the 128-bit data register.

Please replace paragraph [76] in the specification page 16, with the following amended paragraph:

Meanwhile, referring to FIG. 3, the generation of round keys for encryption or decryption required for the encryption and decryption operation of the rijndael block cipher apparatus according to the present invention and performed by the round key generation unit ~~100~~ **110** will be explained.

PAGE 4/18 * RCVD AT 10/23/2008 12:55:39 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/33 * DNIS:2738300 * CSID:312 427 6663 * DURATION (mm-ss):03-16